

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

-----X	
MALIBU MEDIA, LLC,	:
	:
Plaintiff,	:
	:
vs.	:
	:
	:
JOHN DOE subscriber assigned IP address	:
108.30.247.86,	:
	:
Defendant.	:
-----X	

Case No. 1:14-cv-10155-KBF  
Judge Forrest

**PLAINTIFF’S MOTION FOR SANCTIONS**

[Remainder of page intentionally left blank]

## **TABLE OF CONTENTS**

I.	INTRODUCTION .....	4
II.	FACTS .....	5
A.	Defendant Spoiled Material Evidence .....	5
1.	Defendant Had A Duty To Preserve Evidence And Only Defendant Could Have Spoiled It.....	5
2.	Defendant’s Timing Indicates He Acted in Bad Faith.....	6
3.	Defendant Installed, Used, and Deleted Numerous Wiping Software Programs Immediately Before Producing His Drive .....	6
4.	Defendant’s Hard Drive Was Extensively Wiped .....	8
B.	Defendant is Suppressing Evidence .....	9
C.	Defendant Committed Perjury .....	10
1.	Defendant Committed Perjury By Denying the Use of Wiping Software .....	10
2.	Defendant Committed Perjury About His WiFi Password .....	10
III.	ARGUMENT .....	11
A.	Sanctions Are Warranted For Defendant’s Spoliation .....	11
1.	Duty to Preserve Evidence .....	11
2.	Control.....	12
3.	Culpable State of Mind .....	12
4.	Relevance .....	13
B.	Sanctions Are Warranted For Defendant’s Suppression of Evidence.....	13
1.	Sanctions are Mandatory Under Rule 26(g).....	13
2.	Sanctions Are Warranted Under Rule 26(e) and Rule 37. ....	14
C.	Sanctions Are Warranted For Defendant’s Material Perjury.....	14
D.	Terminating Sanctions Are Warranted .....	15
IV.	CONCLUSION .....	17

## **TABLE OF AUTHORITIES**

### **Cases**

<i>ABF Freight Sys., Inc. v. N.L.R.B.</i> , 510 U.S. 317, 323 (1994) .....	15
<i>Arista Records, L.L.C. v. Tschirhart</i> , 241 F.R.D. 462, 465 (W.D. Tex. 2006) .....	16
<i>Capitol Records, Inc. v. Alaujan</i> , 2009 WL 1292977 (D. Mass., 2009) .....	13
<i>Chin v. Port Auth. of N.Y. &amp; N.J.</i> , 685 F.3d 135 (2d Cir.2012) .....	11
<i>Gordon Partners v. Blumenthal</i> , No. 02 CIV 7377 LAK, 2007 WL 1518632 (S.D.N.Y. May 17, 2007) .....	11
<i>Gutman v. Klein</i> , No. 03CV1570(BMC)(RML), 2008 WL 4682208 (E.D.N.Y. Oct. 15, 2008).12, 16	
<i>In re NTL, Inc. Sec. Litig.</i> , 244 F.R.D. 179, 193 (S.D.N.Y. 2007) .....	11
<i>In re Telxon Corp. Sec. Litig.</i> , 2004 WL 3192729 (N.D. Ohio 2004) .....	14
<i>Kosher Sports, Inc. v. Queens Ballpark Co., LLC</i> , No. 10-CV-2618 JBW, 2011 WL 3471508 (E.D.N.Y. Aug. 5, 2011) .....	14
<i>Kronisch v. United States</i> , 150 F.3d 112, 126 (2d Cir.1998) .....	11
<i>Miller v. Time-Warner Commc'ns, Inc.</i> , No. 97 CIV. 7286 (JSM), 1999 WL 739528 (S.D.N.Y. Sept. 22, 1999) .....	16
<i>Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec.</i> , 685 F.Supp.2d 456, 467 (S.D.N.Y.2010) .....	11
<i>Radecki v. GlaxoSmithKline</i> , 646 F. Supp. 2d 310, 315 (D. Conn. 2009) .....	14
<i>Regulatory Fundamentals Grp. LLC v. Governance Risk Mgmt. Compliance, LLC</i> , No. 13 CIV. 2493 KBF, 2014 WL 3844796 (S.D.N.Y. Aug. 5, 2014) .....	11, 12, 13, 15, 16
<i>Reilly v. Natwest Markets Grp. Inc.</i> , 181 F.3d 253, 267 (2d Cir. 1999) .....	15
<i>Residential Funding Corp. v. DeGeorge Fin. Corp.</i> , 306 F.3d 99, 109 (2d Cir. 2002) .....	13

### **Rules**

Fed. R. Civ. P. 26(g)(1)(B)(i) .....	13
Fed. R. Civ. P. 26(g)(3) .....	14
Fed. R. Civ. P. 30(b)(3) .....	13
Fed. R. Civ. P. 34 .....	13

## **PLAINTIFF'S MOTION FOR SANCTIONS**

Pursuant to the Court's inherent authority and Federal Rules of Civil Procedure 26 and 37, Plaintiff moves for the entry of an order sanctioning Defendant for intentionally spoiling material computer evidence, committing perjury and suppressing evidence, and respectfully requests that the Court hold an evidentiary hearing so that it may properly adjudicate this motion.

### **I. INTRODUCTION**

"Based on the timing, there is no doubt that Defendant installed and used file wiping software programs to deliberately destroy evidence in this case." Patrick Paige's Expert Report at ¶ 36 (attached as Exhibit A). "Defendant's statement during his deposition that he 'did not deliberately delete any files' on his Asus computer is perjurious." *Id.* at ¶ 37. "Defendant's deposition testimony that he did not download any computer cleaning software onto his Asus is also perjurious." *Id.* at ¶ 38. According to Mr. Paige, a veteran computer forensics examiner and two time winner of the DOJ's "Outstanding Law Enforcement Officer of the Year" award, "Defendant's Asus had the most file destruction software I have ever seen on one computer." *Id.* at ¶ 35. Indeed, Defendant used eleven different computer software wiping programs to purge his Asus computer of relevant evidence: (1) BCWipe; (2) CyberScrub Privacy Suite; (3) Directory Snoop; (4) Erasure Software; (5) Kill Disk Suite; (6) CCleaner; (7) Wipe MFT; (8) DiskExplorer for NTFS; (9) MooO Disk Cleaner; (10) MooO Anti-Recovery; (11) Asus Secure Delete. *See id.* at ¶¶ 3-8. The wiping software was installed days before Defendant was scheduled to turn over his computer for imaging. And, file deletion software was running the day before Defendant turned his computer over for imaging. *See id.* at ¶ 13. Defendant wiped his computer so clean that only one instance of Defendant's own name can be found on it; and, humorously, that one instance proves Defendant possesses a Kindle Fire that, of course, he failed

to identify or produce. *See id.* at ¶ 25. In total, Defendant failed to produce *at least* eight relevant drives. *Id.* at ¶ 39. Significantly, *while* he was using file destruction software, Defendant plugged in a Western Digital My Passport external drive into his Asus. *Id.* at ¶ 41. “Defendant’s use of a Western Digital My Passport Drive on June 19, 2015, when he was using wiping software, indicates Defendant was making copies of certain data that he wanted to retain prior to or contemporaneously with his using the file deletion software programs to spoil other data contained on the Asus.” *Id.* at ¶ 43.

The prejudice to Plaintiff is obvious. Plaintiff alleges Defendant used his computer, the Internet and BitTorrent to download and distribute pirated copies of Plaintiff’s works. Plaintiff would have found its works on Defendant’s computer. Defendant’s intentional spoliation makes that impossible. In short, Defendant intentionally and with malicious aforethought consciously and deliberately destroyed what Defendant well knew would be the smoking gun. Defendant also lied under oath about the spoliation. And, he lied under oath about the password for his wireless router. For these reasons, Plaintiff respectfully requests that the Court sanction Defendant.

## **II. FACTS**

### **A. Defendant Spoiled Material Evidence**

#### **1. Defendant Had A Duty To Preserve Evidence And Only Defendant Could Have Spoiled It**

On February 27, 2015, Verizon notified Defendant about Plaintiff’s lawsuit. Defendant filed a waiver of service on April 27, 2015. *See* CM/ECF 14. On May 7, 2015, Your Honor denied Plaintiff’s motion for a preservation order because Defendant was *already* under a duty to preserve evidence. Defendant’s attorney also told him “not to delete any files.” Deposition of Defendant, attached hereto as Exhibit “B,” at 163:16-17.

Significantly, Defendant testified that he was the *only* person who used his laptop during the last “couple of months” and that no one else could use it without his “permission.” *Id.* at 210:11-16; 201:5-6. Thus, Defendant is the only person who could have installed, used, and deleted the computer wiping software programs.

## 2. Defendant’s Timing Indicates He Acted in Bad Faith

“Defendant attempted to defraud Plaintiff and the Court by destroying material evidence and I believe Defendant did so because he is likely the infringer.” *Id.* at ¶ 47. Plaintiff’s expert’s conclusion is bolstered by the timing. Indeed, Defendant’s hard drive was originally scheduled to be imaged on June 18, 2015. And, on June 15, 2015, Defendant confirmed that date. However, on June 18, 2015—the morning of the imaging—Defendant rescheduled. Defendant claimed he was “stuck out of town.” Plaintiff acquiesced, and the imaging was rescheduled for Monday, June 22, 2015. Between the 18<sup>th</sup> and 22<sup>nd</sup>, Defendant was obviously very busy deleting and destroying the data on his Asus computer.

## 3. Defendant Installed, Used, and Deleted Numerous Wiping Software Programs Immediately Before Producing His Drive

Patrick Paige’s expert report, at paragraphs 10-23, more fully describes the computer wiping software Defendant used. In short, Defendant used BCWipe—military grade computer file destruction software that is “designed to surgically remove all traces of unwanted files beyond recovery.”<sup>1</sup> Defendant installed BCWipe on June 19, 2015 – three days before he was scheduled to deliver his computer for imaging. Paige Expert Report, at ¶ 13. It was running on June 21. *Id.* It was deleted between or on June 21 and June 22, 2015. *Id.*

Defendant also used:

---

<sup>1</sup> <http://www.jetico.com/products/personal-privacy/bcwipe/> (Last Accessed on September 17, 2015)

- **CyberScrub Privacy Suite**—which is software that deletes “online evidence of ... browsing, it securely deletes various supported applications, Browsers, Windows Sensitive Areas, [and] Peer to Peer activities. It also destroys Emails[.]”<sup>2</sup>
- **Directory Snoop**—which is a search tool that allows Windows users to scan their formatted disk drives to see what data may be hiding.
- **Eraser Software**— which is software that allows a user to “completely remove sensitive data from [a] hard drive by overwriting it several times with carefully selected patterns.”<sup>3</sup>
- **Kill Disk Suite**— which is a software suite used to “wipe all data on hard disks, USB drives and floppy disks completely, [which eliminate] any possibility of future recovery of deleted files and folders.”<sup>4</sup>
- **CCleaner**— which is software that deletes files left by certain programs, including Internet Explorer, Firefox, Google Chrome, Opera, Safari, Windows Media Player, Microsoft Office, Adobe Acrobat, Adobe Flash Player. It also deletes browsing history, cookies, recycle bin, memory dumps, file fragments, log files, system caches, application data, autocomplete form history, and various other data.
- **Wipe MFT**— which is anti-forensic software used to “wipe MFT records and Directory entries which store names, dates, size and other attributes of deleted files.”<sup>5</sup>
- **DiskExplorer for NTFS**— which is software that allows a user to view parts of a hard drive that are not accessible to the average user.
- **MooO Disk Cleaner**— which is file destruction software that can delete “system temporary files, private data in registry, internet browser cache, history and cookies[.]”<sup>6</sup>

---

<sup>2</sup> <http://www.cyberscrub.com/> (Last Accessed on September 17, 2015)

<sup>3</sup> [http://www.freewarefiles.com/Eraser\\_program\\_1793.html](http://www.freewarefiles.com/Eraser_program_1793.html) (Last Accessed on September 17, 2015)

<sup>4</sup> <http://www.killdisk.com/wiper.htm> (Last Accessed on September 17, 2015)

<sup>5</sup> <http://wipe-mft.software.informer.com/> (Last Accessed on September 17, 2015)

- **MooO Anti-Recovery**— which is file destruction software that can “easily erase all the recoverable data from the empty space of your disk drive[.]”<sup>7</sup>
- **Asus Secure Delete**— which is software that uses a “sophisticated technical method” to “permanently delete files.”<sup>8</sup>

There is no evidence that any of the foregoing file wiping software programs existed on Defendant’s Asus computer prior to June 18, 2015 – four days before he was scheduled to deliver his computer for imaging. *Id.* at ¶¶ 10-23. As to many of the programs, the first evidence of their existence is June 19, 2015 – three days before the scheduled imaging. *Id.* All of the file destruction programs were deleted by Defendant prior to his turning over his computer for imaging. *Id.* These programs can be used to permanently delete evidence of BitTorrent use and Plaintiff’s copyrighted works. *Id.*

#### 4. Defendant’s Hard Drive Was Extensively Wiped

Defendant’s testimony establishes that he wiped an enormous amount of data from his hard drive. For example, “Defendant’s name is “NAME.”<sup>9</sup> Yet, a search for the word “NAME” only yields a single result related to a Kindle Fire – which Defendant also failed to produce.” *Id.* at ¶ 25. Defendant testified that he uses his Asus to access his Facebook account. Defendant’s Dep. 75:21-26, 76:2-6. The Asus contains no evidence of Defendant’s Facebook account. Paige Expert Report, at ¶ 26. The same testimony and phenomenon exists with respect to Defendant’s Linkedin account. *Id.* at ¶¶ 27-28. Defendant testified he googled Malibu Media; there is no evidence of this search. *Id.* at ¶ 28. Defendant testified he traveled to Costa Rica, Ghana,

---

<sup>6</sup> <http://www.moo0.com/?top=http://www.moo0.com/software/DiskCleaner/> (Last Accessed on September 17, 2015)

<sup>7</sup> <http://www.moo0.com/?top=http://www.moo0.com/software/AntiRecovery/> (Last Accessed on September 17, 2015)

<sup>8</sup> <http://www.asus.com/support/FAQ/1009738/> (Last Accessed on September 17, 2015)

<sup>9</sup> Redacted pursuant to protective order.



Croatia and Boston; there is no evidence of these trips. *Id.* at ¶¶ 29-32. Defendant’s computer does not contain any personal photos, videos or even a Word document created by Defendant. *Id.* at ¶¶ 33-34. In short, Defendant intentionally wiped his computer almost completely clean.

### **B. Defendant is Suppressing Evidence**

In discovery, Plaintiff asked Defendant to identify every Computer Device used in his home during the preceding two years. *See* Defendant’s Response to Plaintiff’s First Set of Interrogatories, attached hereto as Exhibit “C,” at No. 2. Defendant failed to identify or produce: (1-2) two JetFlash Transcend 32GB USB Devices; (3) a JetFlash Transcend 64GB USB Device; (4) a SanDisk Ultra Fit USB Device; (5) a Generic Flash Disk USB Device; (6) a Verbatim Store N Go USB Device; (7) a Western Digital My Passport 0824 USB Device; and (8) the Kindle Fire, discussed above. *See id.* at ¶ 39. Further, Plaintiff also requested “a complete copy of any external hard drives in Defendant’s possession, custody, or control.” *See* Defendant’s Response to Plaintiff’s First Request for the Production of Documents, attached hereto as Exhibit “D,” at No. 9. Yet, Defendant—again—failed to mention any of the forgoing, and instead falsely stated, “no responsive documents exist.” *Id.* Significantly, all of these devices were connected to Defendant’s laptop during discovery; viz. between and including April 2015 and June 2015. Further, as previously stated, Defendant connected his Western Digital My Passport hard drive to his laptop on June 19, 2015, three days before the rescheduled imaging date. “When he was using wiping software, . . . Defendant was making copies of certain data that he wanted to retain. . . .” Paige Expert Report at ¶ 43. There is simply no reasonable doubt Defendant’s spoliation was intentional. Moreover, “[g]iven the spoliation, the other instances of Defendant’s perjury, I believe Defendant’s failure to identify all relevant drives was

intentional.” *Id.* at ¶ 44. That must be true since Defendant was using these devices during the time he was drafting discovery responses and just prior to imaging.

### **C. Defendant Committed Perjury**

#### **1. Defendant Committed Perjury By Denying the Use of Wiping Software**

Defendant intentionally lied – under oath – about his use of file destruction software:

Q: Have you ever downloaded any kind of software to your laptop for, like, cleaning out files or erasing files or anything like that?  
A: No.

Defendant’s Depo. at p. 80:24-25; 81:2-4. When pressed, Defendant later stated that he installed a “registry cleaner” to “improve” his computer’s performance in 2014. *See id.* at 153: 2-18. There is no evidence of that. Moreover, Defendant perjurally denied “any folder or mass file deletions.” *Id.* at 179:15-16. And, he falsely swore, under oath, that he “did not deliberately delete any files” or remove any software from his laptop other than Avast antivirus software and iTunes. *See id.* at 175:20; 79:13-25; 80:4-14.

#### **2. Defendant Committed Perjury About His WiFi Password**

Unable to keep his story straight, under oath, Defendant told two *completely* contradictory stories about his WiFi security. One *must* be false. Indeed, in his Interrogatory Responses, Defendant swore that “[w]hen Verizon installed the modem, Verizon placed a Verizon-issued password on the device. On or before February 2014, Defendant changed the password to a blank password, and it remained in such state for all relevant times.” *See* Exhibit C, at No. 3. Next, in his deposition, Defendant claimed Verizon *never* placed a password on his Internet, and instead, during March of 2014, Defendant placed the password, “REDACTED”<sup>10</sup> on it. *See* Deposition of Defendant at 52:10-15; 53: 5-14; 57:1-6. These stories cannot coexist.

---

<sup>10</sup> Redacted pursuant to protective order.

“If you tell the truth, you don’t have to remember anything,” said Mark Twain. Defendant is a perjurer who cannot keep his false stories straight.

### **III. ARGUMENT**

#### **A. Sanctions Are Warranted For Defendant’s Spoliation**

“A party to a lawsuit may not destroy relevant evidence without consequence. The nature and magnitude of the consequence follows from the level of culpability.” *Regulatory Fundamentals Grp. LLC v. Governance Risk Mgmt. Compliance, LLC*, No. 13 CIV. 2493 KBF, 2014 WL 3844796, at \*1 (S.D.N.Y. Aug. 5, 2014) (K.B.F.) (imposing terminating sanctions for spoliation). “To support the imposition of sanctions, ‘the innocent party must prove the following three elements: that the spoliating party (1) had control over the evidence and an obligation to preserve it at the time of destruction or loss; (2) acted with a culpable state of mind upon destroying or losing the evidence; and that (3) the missing evidence is relevant to the innocent party’s claim or defense.’” *Id.* (quoting *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec.*, 685 F.Supp.2d 456, 467 (S.D.N.Y.2010), *abrogated on other grounds by Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135 (2d Cir.2012)). Here, Plaintiff easily establishes all of these elements.

##### **1. Duty to Preserve Evidence**

“This obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation—most commonly when suit has already been filed, . . . [or] for example when a party should have known that the evidence may be relevant to future litigation.” *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 193 (S.D.N.Y. 2007) *aff’d sub nom. Gordon Partners v. Blumenthal*, No. 02 CIV 7377 LAK, 2007 WL 1518632 (S.D.N.Y. May 17, 2007) (quoting *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir.1998)). Here, Defendant knew about the

lawsuit no later than February 27, 2015. Further, no later than May 7, 2015 he was expressly advised to preserve evidence. *See* p. 2-3, *surpra*. Thus, when he deleted evidence between July 18-22, 2015, Defendant intentionally and consciously violated his duty to preserve the evidence.

## 2. Control

As explained on p. 3, Defendant had exclusive control over his Asus and is the only possible spoliator.

## 3. Culpable State of Mind

“In this circuit, a ‘culpable state of mind’ for purposes of a spoliation inference includes ordinary negligence. This standard protects the innocent litigant from the destruction of evidence by a spoliator who would otherwise assert an ‘empty head, pure heart’ defense.” *Regulatory Fundamentals Grp. LLC v. Governance Risk Mgmt. Compliance, LLC*, No. 13 CIV. 2493 KBF, 2014 WL 3844796, at \*14 (S.D.N.Y. Aug. 5, 2014). Here, Defendant was not merely negligent, however. Instead, “[b]ased on the timing, there is no doubt Defendant installed and used file wiping software programs to deliberately destroy evidence in this case.” Patrick Paige at ¶ 36. A spoliator’s “bad faith” justifies increased sanctions and when, as here, a spoliator acts “knowingly and intentionally, and then trie[s] to cover it up[,] . . . [such actions] clearly constitute bad faith.” *Regulatory Fundamentals Grp. LLC*, 2014 WL 3844796, at \*15; *see also Gutman v. Klein*, No. 03CV1570(BMC)(RML), 2008 WL 4682208, at \*10 (E.D.N.Y. Oct. 15, 2008) *report and recommendation adopted*, No. 03 CIV. 1570 (BMC), 2008 WL 5084182 (E.D.N.Y. Dec. 2, 2008) (finding bad faith where a party acted in a “concerted effort to scramble the egg, to muddle the hard drive ... just before the court ordered imaging.”).

#### 4. Relevance

“[W]here the computer itself is at the heart of the litigation-where it is, in effect, an instrumentality of the alleged copyright infringement-it is plainly relevant[.]”) *Capitol Records, Inc. v. Alaujan*, 2009 WL 1292977 at \*1 (D. Mass., 2009). Plaintiff respectfully suggests Defendant spoiled his computer with a consciousness of guilt precisely because Plaintiff would have found its works on the Asus. Significantly, when, as here, the evidence is destroyed in bad faith, the Court may assume the evidence is relevant and would have been adverse to the spoliator. *See Regulatory Fundamentals Grp. LLC*, 2014 WL 3844796, at \*14. “When evidence is destroyed in bad faith, that fact alone is sufficient to support an inference that the missing evidence would have been favorable to the party seeking sanctions....” Even if the presumption was not applicable, which it is, “courts must take care not to ‘hold[ ] the prejudiced party to too strict a standard of proof regarding the likely contents of the destroyed [or unavailable] evidence,’ because doing so ‘would subvert the ... purposes of the adverse inference, and would allow parties who have ... destroyed evidence to profit from that destruction.’” *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 109 (2d Cir. 2002).

#### **B. Sanctions Are Warranted For Defendant’s Suppression of Evidence**

##### 1. Sanctions are Mandatory Under Rule 26(g).

Fed. R. Civ. P. 30(b)(3) requires interrogatories be “answered separately and fully in writing under oath.” Implicit in that rule is that the responses not be intentionally perjurious. Fed. R. Civ. P. 34 requires parties to identify and produce the requested documents. Under Fed. R. Civ. P. 26(g)(1)(B)(i) by signing discovery responses, the party certifies the response are “consistent with these rules.” As set forth above, Defendant’s interrogatory responses and responses to document requests were perjurious and intentionally incomplete. When Rule 26(g)

is violated, “the court . . . *must* impose an appropriate sanction[.]” Fed. R. Civ. P. 26(g)(3) (emphasis added).

## 2. Sanctions Are Warranted Under Rule 26(e) and Rule 37.

“Compliance with Rule 37 includes complete and timely supplementation of disclosures and responses in accordance with Rule 26(e).” *In re Telxon Corp. Sec. Litig.*, 2004 WL 3192729 (N.D. Ohio 2004). Rule 26(e) requires a party to “supplement or correct” a response to “an interrogatory, [or] request for production[.]” Rule 37(c)(1) provides: “If a party fails to provide information . . . as required by Rule 26(a) or (e), . . . the court . . . may impose . . . sanctions, including any of the orders listed in Rule 37(b)(2)(A)(i)-(vi).”<sup>11</sup>

Defendant failed to “supplement or correct” his perjurious interrogatory and intentionally incomplete production responses. Indeed, such “responses were intended to mislead [Plaintiff] and conceal the existence of the [evidence].” *Kosher Sports, Inc. v. Queens Ballpark Co., LLC*, No. 10-CV-2618 JBW, 2011 WL 3471508, at \*10 (E.D.N.Y. Aug. 5, 2011) (sanctioning party for non-disclosure). As such, severe sanctions are warranted.

## C. **Sanctions Are Warranted For Defendant’s Material Perjury**

“Perjury is ‘false testimony concerning a material matter with the willful intent to provide false testimony, rather than as a result of confusion, mistake, or faulty memory.’” *Radecki v. GlaxoSmithKline*, 646 F. Supp. 2d 310, 315 (D. Conn. 2009) *aff’d*, 375 F. App’x 46 (2d Cir. 2010). Here, Defendant falsely testified concerning two material matters: (1) the use of file destruction software to erase evidence and (2) his WiFi security, which is material to his claim that someone else used his Internet to commit the infringement. Failing to disclose the file

---

<sup>11</sup> Sanctions under Rule 37(b)(2)(A)(i)-(vi) may include: (i) directing . . . facts be taken as established for purposes of the action, as the prevailing party claims; (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence; (iii) striking pleadings in whole or in part; (iv) staying further proceedings until the order is obeyed; (v) dismissing the action or proceeding in whole or in part; (vi) rendering a default judgment against the disobedient party[.]”

destruction software was intentional – Defendant was using it just before he turned over his hard drive for imaging. Likewise, Defendant told two *completely* contradictory, detailed stories about his WiFi security. As the Supreme Court has observed, “[f]alse testimony in a formal proceeding is intolerable,” and a court “must neither reward nor condone such a ‘flagrant affront’ to the truth-seeking function of adversary proceedings.” *ABF Freight Sys., Inc. v. N.L.R.B.*, 510 U.S. 317, 323 (1994) (citation omitted). Severe sanctions are warranted for Defendant’s material perjury.

#### **D. Terminating Sanctions Are Warranted**

“Whether exercising its inherent power, or acting pursuant to Rule 37, a district court has wide discretion in sanctioning a party for discovery abuses, and for the spoliation of evidence.” *Reilly v. Natwest Markets Grp. Inc.*, 181 F.3d 253, 267 (2d Cir. 1999) (citation omitted). “[A] court should always impose the least harsh sanction that can provide an adequate remedy’ ‘The choices include—from least harsh to most harsh—further discovery, cost-shifting, fines, special jury instructions, preclusion, and the entry of default judgment or dismissal (terminating sanctions).’” *Regulatory Fundamentals Grp. LLC*, 2014 WL 3844796, at \*15 (internal citation omitted). “A spoliation sanction ‘should be designed to: (1) deter parties from engaging in spoliation; (2) place the risk of an erroneous judgment on the party who wrongfully created the risk; and (3) restore the prejudiced party to the same position he would have been in absent the wrongful destruction of evidence by the opposing party.’” *Id.* at \* 12.

Here, terminating sanctions are more than appropriate. Indeed, “[o]ne who anticipates that compliance with discovery rules and the resulting production of damning evidence will produce an adverse judgment, will not likely be deterred from destroying that decisive evidence by any sanction less than the adverse judgment she is tempted to thus evade.” *Arista Records*,

*L.L.C. v. Tschirhart*, 241 F.R.D. 462, 465 (W.D. Tex. 2006); *see also Gutman*, 2008 WL 4682208, at \*12 (“[L]esser sanctions would not adequately deter misconduct of this severity.”) For this reason, courts in this Circuit routinely enter terminating sanctions in factually similar cases. *See Gutman v. Klein*, 2008 WL 4682208, at \*3 (“[L]esser sanctions such as adverse inferences are ill-suited to a case like this, where the spoliator has, in bad faith, irretrievably deleted computer files that likely contained important discovery information.”); *see also Regulatory Fundamentals*, 2014 WL 3844796 (imposing terminating sanctions for the intentional deletion of emails). In *Gutman*—just like here—a forensic expert determined the defendants tampered with a computer to permanently delete files and conceal the dates of the deletions—just days before imaging of the hard drive. *See Gutman v. Klein*, 2008 WL 4682208, at \*12. Because “defendants’ obliteration of the laptop files may well have deprived plaintiffs of crucial evidence[,]” and because “lesser sanctions would not adequately deter misconduct of this severity[,]” the court imposed terminating sanctions, finding “the most serious forms of spoliation merit the harshest sanctions, and in this case, the destruction of evidence was of the worst sort: intentional, thoroughgoing, and (unsuccessfully) concealed.” *Id.*

Defendant’s suppression of material evidence and subsequent perjury further justifies terminating sanctions. *See Miller v. Time-Warner Commc’ns, Inc.*, No. 97 CIV. 7286 (JSM), 1999 WL 739528, at \*3 (S.D.N.Y. Sept. 22, 1999) (imposing terminating sanctions and finding “here [Defendant’s] deliberate attempt to destroy evidence was exacerbated by h[is] repeated perjury on that subject.”). “Blatant and repeated perjury demonstrates such a total disrespect for the Court and the process by which justice is administered that the sanction of [default] is appropriate.” *Id.*



**IV. CONCLUSION**

For the foregoing reasons, Plaintiff respectfully requests that the Court enter a just and appropriate sanction and that it hold a hearing so that it may properly adjudicate this motion.

Respectfully submitted,

By: /s/ Jacqueline M. James  
Jacqueline M. James, Esq. (1845)  
The James Law Firm, PLLC  
445 Hamilton Avenue  
Suite 1102  
White Plains, New York 10601  
T: 914-358-6423  
F: 914-358-6424  
E-mail: jjameslaw@optonline.net  
*Attorneys for Plaintiff*

**CERTIFICATE OF SERVICE**

I hereby certify that on September 22, 2015 I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and that service was perfected on all counsel of record and interested parties through this system.

By: /s/ Jacqueline M. James